SEPS

Space Equipment Planning System

Questions or comments related to this plan should be directed to:

Contingency Plan Point of Contact:

John Hallahan
Logistics
Phone: 703/575-2391
Email: john.hallahan@tma.osd.mil

DMFO

SPACE EQUIPMENT PLANNING SYSTEM (SEPS) VERSION 1.0

YEAR 2000 CONTINGENCY

AND

CONTINUITY OF OPERATIONS PLAN

VERSION 3.0

Dated: May 7, 1999

TABLE OF CONTENT

1.0 Introduction

This Y2K Programmatic Contingency Plan is developed to ensure Y2K compliance is achieved for SEPS as quickly and efficiently as possible. The objectives of this plan are:

- Document SEPS Y2K programmatic risk assessment
- Present performance/technical risks and contingency plans to assure continuity of SEPS operations on schedule and within budget
- Present a programmatic zero-day strategy.

The scope, size and stability of SEPS, and the nature of the system, are such that the separate preparation and implementation of a risk control schedule is not considered to be either cost-effective or warranted. No revised system deployment is planned for SEPS specifically for the purpose of resolving Y2K issues. If there is a Y2K problem or question, the following individuals will address your this system requirements:

Point of Contract (Priority Listing):

Primary POC – Ms. Carol Monnin (703) 845-3863
Secondary POC - John Durgavich (703) 681-2677
Third POC - Ms. Cleo Manspile (703) 681-3966

2.0 Programmatic Risk Assessment

A programmatic risk assessment was conducted and documented using the questionnaire presented in Figure 1. Programmatic risk assessment evaluates risks in the areas of cost, schedule, and technical performance. Significant conclusions reached during the risk assessment include:

- Cost Risks. No significant cost risks are perceived for FY1999 or FY2000.
- No significant dependencies/interdependencies exist with other automated information systems (AISs).
- The risk associated with loss of data exchange is non-existent since the current version of SEPS operates without automated data exchange. Procedures are in place by which data can be reconstituted if required.
- Schedule risks are minimal.
- Risk control measures have been developed and are documented in this plan.
- No specific risk control schedule is required.
- Performance/Technical Issues. Minimal performance and technical risks are perceived. Risk mitigation strategies are presented in this plan.

3.0 Cost and Technical Risk Management

No significant Cost or Technical risks have been identified. Contingency measures to continue operation are identified in this plan. The results of this analytical process are documented in Figure 1 Y2K Programmatic Risk Assessment Questionnaire.

Y2K Programmatic Risk Assessment Questionnaire	
AIS: SEPS	**Date: 8/24/98**
Cost Risk Evaluation	
1. Has the renovation/validation of the system or replacement system been fully funded? **YES** 2. Does the funding include the deployment, testing, implementation, training, and conversion of the new or renovated system? **No new or renovated system is planned.** 3. Has the cost of ensuring Y2K compliance of the operating system software and hardware been funded? **YES** 4. Have all interfaces (internal and external) been identified and has sufficient funding been earmarked to ensure renovation, testing, and certification, as required? **SEPS has no external interfaces** 5. Are contingency funds available to cover unanticipated renovation, testing, and/or implementation issues? **NO.**	
Rating: High Risk Medium Risk ***Low Risk***	
Schedule Risk Evaluation	
1. Have all DoD and MHS mandated phase milestones been achieved? * **YES** 2. Is implementation going to be achieved within DoD and MHS mandates? * **N/A** 3. Have testing and rework activities been factored into the schedule? **N/A** 4. Have interface renovations/development (internal and external) been factored into the schedule? **N/A** 5. Has sufficient time been scheduled for interface testing, rework, and certification? **N/A** *6.* Are there significant schedule interdependencies with other AIS projects? **NO** 7. Are there significant schedule interdependencies with system software, hardware, or infrastructure elements? **NO** 8. Are COTS vendor schedules adequate to meet DoD and MHS requirements? **YES** 9. Has a master program schedule network been developed in an automated project management tool? **N/A** 10. Has a critical path been identified and has critical path analysis been performed? **N/A** ***** If the answer to question 2 is NO schedule risks must be classified as high.	
Rating: High Risk Medium Risk ***Low Risk***	
Performance/Technical Risk Evaluation	
1. Has a formal Y2K Project Plan been prepared, approved, and published? **IN PROCESS** 2. Does the project plan address system software and system-to-system interfaces? **N/A** 3. Does the plan address local area/wide area communications? **N/A** 4. Does the plan address data conversion, testing, training, and certification requirements? **YES** 5. Has the local area communications system (LAN) been determined compliant? **N/A** 6. Does the plan include procedures for ensuring Y2K compliance of executive software and hardware? **YES** 7. Does the plan call for system-level testing to include COTS products and internal and external interfaces? **YES**	
Rating: High Risk Medium Risk ***Low Risk***	

Figure 1

SEPS Programmatic Risk Assessment Questionnaire

Risk	Risk Mitigation Methods
Performance/Technical Risks	
Performance/Technical Risk 1: SEPS does not achieve Y2K compliance on-time as scheduled. System will not function properly or as intended.	• Will implement system on schedule, with supplemental manual procedures. • Interim procedures developed and ready to implement. • Coordinating with appropriate project manager to remain current of schedule issues.
Performance/Technical Risk 2: Failure of wide area communications infrastructure to support data gathering from interfacing systems (data needed for system to function properly).	• Not in scope of SEPS.
Cost Risks	
Cost Risk 1: Potential for inadequate funding for extensive re-testing	• Will advise of additional funding requirements as identified. None anticipated at this time. • Will identify and reprogram additional funds from internal sources, if needed.
Cost Risk 2: Potential for inadequate funding to re-establish failed interfaces.	• None – no external interfaces.

Figure 2

SEPS Cost and Technical Risk Management

4.0 SEPS System-Level AIS Contingency Plan

SEPS System-Level Contingency Plan					
Normal Operating Procedures	Risk	P^o	C^o	RC	Contingency Operations Mode
Problem Identification					
1. User reports problem by calling system help desk.	Local help desk unable to resolve.	M	H	H	User implements partial/full contingency operating mode (e.g., manual support of business process). Help desk notifies SEPS Maintenance Team (contractor support). User advised of workaround or advised to stand down until problem is resolved.
Problem Analyses					
1. Maintenance Team resolves problem, provides fix guidance to site.	Maintenance Team unable to resolve problem.	M	H	H	Maintenance team conducts analysis – implements steps 2,3 or 4 as appropriate.
2. Maintenance Team refers problem to vendor.	Vendor unable to solve problem in a timely manner.	L	M	M	Implement contract/delivery order to conduct problem analyses. Use vendor developmental environment, as arranged.
3. Coordinate non-software problems with contractors/vendors	Failure of outside party to accept problem ownership or co-ownership.	L	M	M	Implement problem escalation procedures in MOU/A(s). Clearly define what constitutes problem ownership/co-ownership in MOU/As.
4. Determine if problem is caused by hardware, system software, or local/wide area communications.	Failure to identify problem	L	M	M	Implement contract/delivery order to conduct problem analyses. Use vendor developmental environment
Software Repair/Problem Resolution					
1. Maintenance Team repairs problem, provides fix to user.	Unable to resolve, not an AIS problem	L	M	M	Identify/notify interfacing organization/project, as required.
2. Maintenance Team repairs problem, provides fix to user.	Unable to resolve, hardware problem	L	M	M	Exercise pre-existing written agreements with hardware vendor to repair and distribute/deploy repair.
3. Maintenance Team repairs problem, provides fix to user.	Unable to resolve, local/wide area communications problem.	L	M	M	Identify/notify interfacing organization/project, as required
4. Maintenance Team repairs problem, provides fix to user.	Unable to resolve, system SW issue.	L	M	M	Exercise repair agreement(s) with vendor(s) to affect repair.
Software Distribution					
1. Maintenance Team distributes software fix via U.S. Mail distribution of diskette/CD-ROM.	U.S. Mail too slow to meet distribution requirements.	L	L	L	Use express mail, e-mail options, as appropriate. Validate data recovery procedures during testing, and include instructions for data recovery.
2. Hardware fix implemented by vendor.	Vendor is overrun with Y2K problems.	L	H	H	Exercise agreement(s) for vendor(s) or alternate sources to conduct on-site repair and implementation.

5.0 SEPS Trigger Identification

This section is provided to describe what visible symptoms may be observed in the event of a SEPS Y2K failure and to outline the procedures to be followed by the user in the event that these symptoms are encountered. A copy of a draft information to SEPS users is provided as Appendix A to this document. This document contains this information.

SEPS Trigger Identification	
Symptom	Response
Report dates incorrect. (SEPS uses the system date on the cover page of its reports.)	Any observed anomaly should be reported to the SEPS help desk *only after the user has verified that the system date is correct on the computer desktop.* If the desktop data is not correct, the user should contact the IS support center for a resolution to this problem; this is not a SEPS issue.
Displayed dates (e.g. for last update of projects) will be incorrect or will be incorrectly formatted.	The user should contact the SEPS Help Desk.
Phase data is incorrect (for those projects with multiple phases).	The user should contact the SEPS Help Desk and request that they notify the SEPS development team. This may be a design issue.

6.0 SEPS Alternate Procedures

The SEPS application *per se* does not currently include a data exchange method. No alternate operating procedures to perform SEPS functions are available or planned. This section identifies the data exchange manual processes currently used for SEPS. One process, the creation of project transfer files (ZIP format), is supported by SEPS.

SEPS Alternate Procedures	
Data	Data Exchange Method
Transfer of Project Data	Data exchange of SEPS data is accomplished by transferring copies of files. The transfer mechanism is either: • Creating floppy disk copies (also ZIP files used for SEPS project transfer) • Placing copies of files in common accessible areas (e.g. shared network areas) • E-Mail None of these processes is under SEPS' control.

7.0 SEPS Zero-Day Strategy

The objective of this zero-day strategy is to ensure the project office is ready to provide responsive management and control of problem scenarios immediately before, during, or immediately after the beginning of fiscal or calendar year 2000. This strategy includes prior testing, issuance of user instruction on methods of saving data and user instruction on recognizing SEPS Y2K problems should they occur. Current SEPS resources will be sufficient to support this effort; no resource augmentation is contemplated.

SEPS Programmatic Zero-day Strategies	
Planning Element	Elements of Zero-day Strategy
Staff resource assignments	• Include Y2K zero-day support tasking in written task statements/delivery orders with system developer and support contractor. • Familiarize help desk personnel with the elements of the SEPS System-Level Contingency Plan.
General Readiness	• Include in task statement/delivery order for FY99 that a development environment will be available for repairing and testing Y2K related system failures (This will be the same as the current development environment). • Include language requiring support contractor and vendor to devote development personnel to Y2K-related problem analysis and repair. • Develop and publish zero-day strategy. • Advise users of methods to safeguard data and how to test for Y2K problems. (Note: Draft of instructions to users is included as Appendix A to this document) • Implement test scenarios. • Conduct Y2K test and verify results data.
Ongoing Communications	• Validate POCs prior to first week of November 1999. • Review lines of communications with the user community the prior to last week of November 1999. • Issue Y2K bulletins to user community during November 1999. Advise user community of current POC list, problem reporting procedures, and other topics deemed appropriate.
Project schedules	• For each problem event, a task will be entered into the SEPS Problem/Resolution List. • Advise the SEPS Tri-Service Committee of all problem/resolution status.

Zero-day Strategy

8.0 SEPS Problem Reporting Procedures

This section is provided to restate the procedures available to SEPS users for reporting problems. As SEPS currently has Help Desk Support, no alternate or additional problem reporting procedures are planned.

SEPS Problem Reporting Procedures	
Problem	Procedure
All problems.	User reports problem to the SEPS Help Desk. Help Desk makes an initial determination as to whether the problem is Y2K-related. ('Trigger' list in Section 5, above.) If Y2K problem, Help Desk contacts developer personnel.

9.0 SEPS Data Preservation Procedures

This section is provided to restate the procedures available to SEPS users for preserving and safeguarding data. Much of this information duplicates standard data safety practices, however SEPS users have one additional method of saving data provided through the system.

SEPS Data Preservation Procedures	
Data Type	Method
Project Files	• Network Backup (Standard windows data copy procedures) • Save as ZIP transfer files (SEPS function – instructions in SEPS' Help) onto network and diskette
Back-up Procedures for Calendar Year rollover and Leap Year	• Network Backup (Standard windows data copy procedures) • Save as ZIP transfer files (SEPS function – instructions in SEPS' Help) onto network and diskette • Review back-up file to ensure back-up procedure was successful. • Store back-up files in a secure location
Reference Files (Criteria)	Users not required to back up these files. Backup is at HA.
SEPS Application	Users not required to back up these files. Backup is at HA.

10.0 SEPS Y2K Resource Planning

This section is provided to identify the resources anticipated to be required, over and above the resources currently dedicated to SEPS development and support, for Y2K activity.

SEPS Y2K Resources		
Requirement	Resources Required	Duration
Help Desk Support	Help Desk Personnel. Ensure Help Desk personnel available during weeks 1 and 2 of January, 2000. No additional support required. Current Staff is sufficient. No Help Desk on Saturday, January 1 or Sunday, January 2.	2 weeks
Development personnel support	Developers. Ensure Developers available during weeks 1 and 2 of January, 2000. No additional support required. Current Staff is sufficient.	2 weeks

Appendix A

User Information For SEPS Y2K

This appendix contains a draft of a letter to be provided to the SEPS Service Points Of Contact for dissemination to SEPS users on or about mid-October, 1999.

Included are:

- recommendations for preparation for Y2K
- data preservation
- data recovery
- recognition of Y2K errors in SEPS
- trouble reporting

This document will be revised as required prior to dissemination.

Y2K Continuity Of Operations Procedures for SEPS

Point of Contract (Priority Listing):
Primary POC – Ms. Carol Monnin (703) 845-3863
Secondary POC - John Durgavich (703) 681-2677
Third POC - Ms. Cleo Manspile (703) 681-3966

Background

SEPS Version 1.00 has been tested and checks out as Y2K compliant. The information below is intended to provide an additional measure of assurance that unforeseen circumstances stemming from Y2K will not pose any threat to SEPS data.

Recommended User Preparation

The following are recommended before January 1, 2000. Most of this is common sense and will likely be redundant with recommendations associated with other systems and office business processes.

1) Prior to January 1, 2000, but as close as possible to the last working day of Calendar 1999, back up SEPS projects. This may be accomplished in one of two ways:

   - If the System is connected to a network, use the network facilities to save the project files. These files will generally be found in a series of subdirectories of the / SEPS/ Projects directory. Save the projects subdirectory in its entirety, with all of its subdirectories, in a separate directory. Record the directory path where the projects are backed up.
   - If the system is installed in a standalone configuration, use the SEPS project transfer function to create project transfer files. Instructions for this process are in SEPS Help. As the SEPS transfer function creates ZIP files, each project should occupy no more than one floppy disk.

   If assistance and guidance is needed in these procedures, contact the SEPS Help Desk.

2) Verify that your computer has been certified as Y2K compliant. Generally, there will be a sticker affixed to the front of the computer case with this certification. If your computer has not been certified, contact your IS support center and request that they do so. *Do not contact the SEPS Help Desk; this is not a SEPS issue.* However, if your computer has not been certified compliant, or has failed certification, it is more critical that you perform the backup procedures above.

3) Create a sample report(s) for one or more projects. This will be used for comparison purposes during January, 2000. Create this report (or these reports) using data from a project that you do not plan to change. The Program For Design (PFD) report and the Equipment Summary report (for projects having Equipment Plans) comprise a reasonably good workout for SEPS.

Zero Day (January 3, 2000)

There is no current plan for SEPS assistance to be available on Saturday, January 1, 2000 or on Sunday, January 2, 2000. If you anticipate a requirement to use SEPS on those days, please contact the SEPS Help Desk and inform them of this requirement and the justification for it so that the necessary support personnel may be made available. Normal Help Desk and developer assistance will resume on Monday, January 3, 2000, the first normal working day of the New Year.

There is no alternative or work-around for SEPS functions. However, neither is SEPS a life support or time-critical system.

On January 3, 2000, the SEPS development team will retest SEPS in a normal operating configuration to determine if there have been any unforeseen effects from Y2K problems. This test will be conducted on a

Windows NT 4.0 platform and will include creation of new projects and repeat testing of reports from prior projects. Users will be immediately notified if any problems are observed. This test is anticipated to be complete by 12:00 noon, EST.

For users, the following are recommended:

1) Start SEPS as you normally would. Do not restore from backup, but run normally. Any problems stemming from Y2K will be evident in one of three areas:

   - Report dates will not be correct. SEPS uses the system date on the cover page of its reports. Any observed anomaly should be reported to the SEPS help desk *only after you have verified that the system date is correct on the computer desktop.* If the desktop data is not correct, contact your IS support center for a resolution to this problem; this is not a SEPS issue.
   - Displayed dates (e.g. for last update of projects) will be incorrect or will be incorrectly formatted. If you observe this, contact the SEPS Help Desk.
   - Phase data is incorrect (for those projects with multiple phases). Contact the SEPS Help Desk with a request that they notify the SEPS development team.

2) Rerun the sample reports you prepared last year and compare the results. If there have been no changes, made to the project data, the reports should be the same, except for the report date.

3) Should you observe a problem in any of these areas, contact the SEPS Help Desk before attempting to restore from backup. You may be requested to forward a copy (or a sample) of your backup files to one of the Development Team members for a trial of the data restore procedures.

Restoring Project Data From Backup

For restoring data from file backup, the SEPS Help Team or SEPS Development Team may recommend one of two methods:

- Re-pointing SEPS to the directory where the backup is located. This capability is provided within SEPS and the procedure for doing this is in the SEPS Help File.
- Completely copying the backup data, overwriting your project directory and all of its subdirectories. *This is not preferred, as all changes made since the backup will be lost*.

For rebuilding project data from transfer files, it is recommended that each project be rebuilt under a different name in a different directory. The procedure for doing this is in the SEPS Help File.

Contact the Help Desk before undertaking any of these procedures. It may be necessary to 'dry run' the process to ensure success.

Summary

Although SEPS is designed to be immune to Y2K effects and has been tested to the extent that it is possible to do so, it is not possible to assert with 100% certainty that SEPS will suffer no effect. The procedures outlined above comprise a very conservative approach to assure that no project data is compromised in any way. Your cooperation is appreciated.